UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

SHARYL THOMPSON ATTKISSON, JAMES HOWARD ATTKISSON, SARAH JUDITH STARR ATTKISSON, Plaintiffs, v. UNITED STATES OF AMERICA, FEDERAL BUREAU OF INVESTIGATION, MCI COMMUNICATIONS SERVICES, INC. d/b/a VERIZON BUSINESS SERVICES, CELLCO PARTNERSHIP d/b/a VERIZON WIRELESS, VERIZON VIRGINIA, LLC, UNKNOWN NAMED AGENTS OF THE DEPARTMENT OF JUSTICE, in their individual capacities, UNKNOWN NAMED AGENTS OF THE UNITED STATES POSTAL SERVICE, in their individual capacities, UNKNOWN NAMED AGENTS OF THE UNITED STATES, in their individual capacities, Defendants.	Civil Action No. 1:17-cv-364-LMB

PLAINTIFFS' FIRST AMENDED CONSOLIDATED COMPLAINT

Plaintiffs, by and through undersigned counsel, submit the following Amended

Complaint.

1. Counts 1 and 2 are brought pursuant to *Bivens*[1] and challenge Defendants' unauthorized and illegal surveillance of Plaintiffs' laptop computers and telephones from 2010-2014 under the First Amendment to the United States Constitution and the Fourth Amendment to the United States Constitution. Counts 3 through 8 are brought through and pursuant to the Federal Tort Claims Act ("FTCA"), 28 U.S.C. § 2671 *et seq*., the United States Constitution, and the law of the Commonwealth of Virginia.

2. The FTCA is the exclusive remedy against the United States for certain negligent or wrongful acts of federal employees acting within the scope of their employment. See 28 U.S.C. § 2679(b)(1); *Aliota v. Graham*, 984 F.2d 1350, 1355 (3d Cir. 1993). The FTCA "operates as a limited waiver" of the sovereign immunity of the United States.

3. This action is also brought under the United States Constitution pursuant to *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971), for the defendants' warrantless searches and seizures in violation of the First and Fourth Amendments; unlawful search and seizure of Plaintiffs' home, private papers, information, communications, and belongings in violation of their Fourth Amendment rights; and attack on First Amendment rights as a journalist engaged in her profession.

JURISDICTION

4. The subject litigation arises under the Constitution and laws of the United

---

[1] *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics,* 403 U.S. 388 (1971). *Bivens* action is now regarded as the federal equivalent to 42 U.S.C. § 1983, which permits state officials to be sued for violations of individuals' constitutional rights.

States, and the Court has jurisdiction over the subject matter of this Complaint under 28 U.S.C. §§ 1331 & 1346(b); *Bivens*; the Federal Tort Claims Act, 28 U.S.C. § 2671 et seq.; 42 U.S.C. § 1983; and 18 U.S.C. §§ 3142, 3144. See *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971). The Court has jurisdiction under 28 U.S.C. § 1331; 28 U.S.C. § 1343; 28 U.S.C. § 1346; 28 U.S.C. § 2201; and 28 U.S.C. § 2202.

5. On December 26, 2014, Plaintiffs submitted an Administrative Tort Claim to the United States Department of Justice and the United States Postal Service as required by law. Plaintiffs' claim was deemed denied by virtue of Claimants/Plaintiffs receiving no response from the respective federal agencies within six months of filing, pursuant to 28 U.S.C. § 2675(a). Plaintiffs have therefore exhausted all available administrative remedies, and satisfied all conditions precedent, to the filing of suit.

6. Venue is proper in this District because a substantial part of the events complained of and giving rise to Plaintiff's claims occurred in this District. See 28 U.S.C. §§ 1391(b), 1391(e), 1402(b).

PARTIES

7. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein, including the allegations in the original complaint.

8. At all times relevant to the subject lawsuit, separate Plaintiff Sharyl Attkisson is, and was, a citizen and resident of Leesburg, Virginia, and an investigative reporter for CBS News. Plaintiff was responsible for investigating, writing, publishing, and airing investigative news stories on a wide-variety of topics, including the federal

gun-trafficking investigation that came to be known as *"Fast and Furious,"* and the controversial attack against the American diplomatic mission in Benghazi, Libya, by the Islamist terrorist group Ansar al-Sharia.

9. At all times relevant hereto, Ms. Attkisson was a member of "the press" as described by the First Amendment to the Constitution of the United States. In the course of her investigative journalism, she experienced confrontational encounters with officials within the DOJ and White House who demanded disclosure of the identity of confidential sources who might have been leaking information. For example, Federal agencies and the White House repeatedly withheld unclassified documents that were in the public interest, at times invoking "national security" as justification.

10. During the same time period, DOJ vastly expanded its offensive cyber-security capabilities, efforts, technologies and resources in the name of national security, including the extraordinary decision to actively target journalists and news organizations with electronic surveillance as part of leak investigations. The FBI was the primary DOJ agency tasked with carrying out these national security investigations, using a combination of legal and illegal means.

11. Here, because Plaintiff Sharyl Attkisson's investigative reporting truthfully and authentically revealed the failings of many of the Obama Administration's policies and programs, she and her family, at her work and in their home, were subjected to the full panopticon of the Federal government's electronic surveillance and cyber-stalking capabilities. As discussed in detail below, the FBI—with authorization and political cover from DOJ, and support from other government agencies and commercial

organizations—carried out a multi-year advanced persistent threat ("APT") cyber-attack against Plaintiffs. For example, Plaintiff Sharyl Attkisson discovered that her computers and telephone had been hacked or compromised remotely, and that an unauthorized party or parties had illegally infiltrated her electronics and placed software on her laptop computer, and that her confidential, professional, and personal information had been illegally accessed, compromised, and infiltrated.

12. At all times relevant to the subject lawsuit, Plaintiff James Howard Attkisson is and was a citizen and resident of Leesburg, Virginia, and was married to Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at Ms. Attkisson's residence, Mr. Attkisson was subjected to surveillance as well, and his confidential, professional, and personal information was illegally accessed.

13. At all times relevant to the subject lawsuit, Plaintiff Sarah Judith Starr Attkisson was a citizen and resident of Leesburg, Virginia, and the daughter of James and Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at Sarah Attkisson's residence, she was subjected to surveillance as well, and her confidential, professional, and personal information were illegally accessed.

14. Defendant UNITED STATES is sued under the Federal Tort Claims Act, 28 U.S.C. § 1346, for the tortious acts of its employees.

15. Defendant FEDERAL BUREAU OF INVESTIGATION ("FBI") is the agency within the Department of Justice responsible for gathering intelligence for material witness and criminal proceedings, seeking warrants, executing arrests, and administering certain databases that contain and are used to disseminate arrest, detention and other

records.

16. Defendant MCI COMMUNICATIONS SERVICES, INC., is a Delaware corporation doing business as "Verizon Business Services." Verizon Business Services is a telecommunications service provider headquartered in Ashburn, Virginia, and its ultimate parent is Verizon Telecommunications, Inc. ("Verizon") (NYSE:VZ), a publicly-traded telecommunications holding company. Verizon Business Services offers long-distance, local, wireless telecommunications, and information technology services.

17. Defendant CELLCO PARTNERSHIP is a Delaware partnership doing business as "Verizon Wireless." Verizon Wireless is a wireless communications services and products company headquartered in Basking Ridge, New Jersey, and its ultimate parent is Verizon. Verizon Wireless was formed in 2000 as the result of a joint venture between Verizon and Vodafone Group, Plc. ("Vodafone"). In September 2013, Verizon acquired all of Vodafone's interest in Verizon Wireless.[2]

18. Defendant VERIZON VIRGINIA LLC ("Verizon–VA") is a Virginia limited liability company headquartered in Falls Church, Virginia, and its ultimate parent is Verizon. Verizon–VA provides domestic wireline telecommunications services, including its FiOS fiber-to-the-premises services for residential and small business subscribers, in the local access and transport areas ("LATA") of Virginia.

19. While Plaintiffs have been able to identify some of the Unknown Named

---

[2] Verizon Communications, Inc., Form 10-K filing to the US Securities and Exchange Commission, Feb. 21, 2017, available at https://www.sec.gov/Archives/edgar/data/732712/000119312517050292/d296602d10k.htm

Agents of the Department of Justice, United States Postal Service, and of the United States of America, Plaintiffs are unaware of the true names and capacities, whether individual or otherwise, of all of the Unknown Federal Agents referenced in the caption and therefore sue the unnamed Defendants by fictitious names. Plaintiffs are informed and believe, and on that basis, allege, that these Defendants, and each of them, are in some manner responsible and liable for the acts and/or damages alleged in the Complaint, and that these Defendants, including all Defendants, are and were employees or agents of the federal government who acted under color of law, and that each subjected Plaintiffs to, or caused them to be subjected to, constitutional violations and damages from Defendants' tortious actions.

BACKGROUND

20. The First Amendment protects the rights of American citizens to engage in free and open discussions, and to associate with persons of their choosing, and the Fourth Amendment guarantees that citizens will be free of unreasonable searches and seizures. Defendants herein have expressly interfered with those rights. More importantly, Defendants alleged activities in the aggregate have served to deter the exercise of First Amendment rights by those who become aware of the covert operations.

21. The facts alleged herein, and those referenced from public sources, demonstrate a clear and present danger to our most fundamental protections as a result of an intelligence community employing surreptitious collection techniques, including highly sophisticated forms of electronic surveillance, to achieve overly broad intelligence targeting and collection objectives in violation of law.

22. During all times relevant to the subject Complaint, Ms. Attkisson was an investigative reporter for CBS News. She served CBS for twenty (20) years. Her job required her to investigate and report on national news stories. In 2011, during the course of her reporting, Plaintiff Sharyl Attkisson began investigating what later became known as the *"Fast and Furious"* gun-walking story[3] involving federal agents from the Bureau of

[3] The "Gun-walking", or "letting guns walk", was a tactic of the United States Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), which ran a series of sting operations between 2006 and 2011 in the Tucson and Phoenix area where the ATF purposely allowed licensed firearms dealers to sell weapons to illegal straw buyers, hoping to track the guns to Mexican drug cartel leaders and arrest them. The operations were done under the umbrella of "*Project Gunrunner*," a project intended to stem the flow of firearms into Mexico by interdicting straw purchasers and gun traffickers within the United States. The Jacob Chambers Case began in October 2009 and eventually became known in February 2010 as "Operation *Fast and Furious*" after agents discovered Chambers and the other suspects under investigation belonged to a car club.

The desired goal of allowing these purchases was to continue to track the firearms as they were transferred to higher-level traffickers and key figures in Mexican cartels, with the expectation that this might lead to arrests and dismantling of the cartels. The tactic was questioned during the operations by a number of people, including ATF field agents and cooperating licensed gun dealers. During Operation *Fast and Furious*, the largest gun-walking probe, the ATF monitored the sale of about 2,000 firearms, of which only 710 were recovered as of February, 2012. A number of straw purchasers were arrested and indicted; however, as of October, 2011, none of the targeted high-level cartel figures had been arrested. Guns tracked by the ATF were found at crime scenes on both sides of the Mexico–United States border, and the scene where United States Border Patrol Agent Brian Terry was killed in December, 2010.

The "gunwalking" operations became public in the aftermath of Terry's murder. Dissenting (whistleblowing) ATF agents came forward to Congress in response. According to Humberto Benítez Treviño, former Mexican Attorney General and chair of the justice committee in the Chamber of Deputies, related firearms were found at numerous crime scenes in Mexico where at least 150 Mexican civilians were maimed or killed. Revelations of gun-walking led to controversy in both countries, and diplomatic relations were damaged. As a result of a dispute over the release of Justice Department documents related to the

Alcohol, Tobacco, and Firearms (ATF) improperly permitting weapons to pass into the hands of the Mexican drug cartels.

23. Plaintiff Sharyl Attkisson's first *Fast and Furious* report aired on CBS on February 22, 2011. The report quoted and relied upon numerous confidential sources, all of whom were critical of the *Fast and Furious* gun-walking strategy deployed by the respective federal agencies.

24. In February 2011, the ATF, in an internal memorandum, instigated an orchestrated campaign against Plaintiff Sharyl Attkisson's CBS News reporting, including efforts to discredit it, and outlined a strategy for the ATF to push "positive stories" in order to "preempt some negative reporting."[4]

25. Despite the foregoing efforts, Plaintiff Sharyl Attkisson continued to report *Fast and Furious* stories. When contacted for comment, DOJ officials persisted in their denial of the allegations and continued efforts to unveil her confidential sources. ATF

---

scandal, Attorney General Eric Holder became the first sitting member of the Cabinet of the United States to be held in contempt of Congress on June 28, 2012. Earlier that month, President Barack Obama had invoked executive privilege for the first time in his presidency over the same documents.

[4] See Sharyl Attkisson, *ATF Memo After CBS Report: We Need Positive Press*, CBS News, Mar. 4, 2011, online at http://www.cbsnews.com/8301-31727_162-20039251-10391695.html (last visited on Feb. 2, 2017).

> "Given the negative coverage by CBS Evening News last week and upcoming events this week, the bureau should look for every opportunity to push coverage of good stories. Fortunately, the CBS story has not sparked any follow up coverage by mainstream media and seems to have fizzled….It was shoddy reporting… ATF needs to proactively push positive stories this week, in an effort to preempt some negative reporting, or at minimum, lessen the coverage of such stories in the news cycle by replacing them with good stories about ATF."

sources told her that the Agency was actively seeking to identify government insiders who wereproviding information or "leaking" to her and CBS.

26. In September 2011, Plaintiff Sharyl Attkisson reported on secret audio recordings that implicated the FBI in an alleged discrepancy in its accounting of evidence in the *Fast andFurious* related murder of Border Patrol Agent Brian Terry.

27. The referenced reporting by Plaintiff Sharyl Attkisson was public reporting for CBS News and available both on television and online.

28. Also, in September 2011, Plaintiff Sharyl Attkisson reported on the alleged involvement of an FBI informant in the *Fast and Furious* matter.

29. In October 2011, Plaintiff Sharyl Attkisson reported on the continuing controversy regarding the FBI's accounting of evidence in *Fast and Furious.*

30. In November 2011, Plaintiff Sharyl Attkisson reported on evidence contradicting Attorney General Holder's sworn testimony wherein he claimed that he had only heard of *Fast and Furious* for the first time in the past couple of weeks.

31. In mid-to-late 2011, Plaintiffs began to notice anomalies in numerous electronic devices at their home in Virginia. These anomalies included a work Toshiba laptop computer and a family Apple desktop computer turning on andoff at night without input from anyone in the household, the house alarm chirping daily at different times, often indicating “phone line trouble,” and television problems, including interference. All of the referenced devices use the Verizon FiOS line installed in Plaintiffs’ home. Yet, Verizon was unable to cure the problems, despite multiple attempts over a period of more than a year.

32. In December 2011, Plaintiff Sharyl Attkisson reported on the DOJ's

formal retraction of a letter and a misrepresentation made to Congress in February 2011, which had stated, incorrectly, there had been no gun-walking.

33. In January 2012, Plaintiff Sharyl Attkisson contacted Verizon about ongoing Internet problems and intermittent connectivity because the FiOS residential internet service began constantly dropping off. She had not experienced similar problems previously. In response to the complaint, Verizon sent a new router, which was immediately installed at Plaintiffs' home. However, the new router failed to resolve the issues.

34. In January 2012, Plaintiff Sharyl Attkisson began a series of reports for CBS News, spanning several months, which were critical of the Obama Administration's "green energy" initiatives, including the Executive Branch's failed investment in solar-panel manufacturer Solyndra.

35. In February 2012, an unauthorized party or parties remotely installed sophisticated surveillance spyware on Ms. Attkisson's Toshiba laptop. The invasion was obviously unknown to Ms. Attkisson at the time, but revealed later by forensic computer analysis, including factual evidence demonstrating that Plaintiffs' computer systems were targets of unauthorized surveillance efforts, including prolonged ongoing surveillance of the iMac. From artifacts remaining on the iMac, the intrusions were occurring as early as June 2011.

36. The forensic analysis likewise revealed direct targeting of Plaintiff Sharyl Attkisson's Blackberry mobile phone when connected to her personal Apple iMac computer in Plaintiffs' Leesburg, Virginia home. Operating system log files reveal a file recovery process performed by an intruder that transferred large numbers of records off the

BlackBerry. Changes to VPN settings were likewise found as the enabling of the built in Ethernet connection, after years of not being used, reflect further clear evidence of unauthorized surveillance activities. The issuing of the *smbclient* command along with recovered records showing the iMac mounted as a network shared resource, is further evidence of uninvited, remote surveillance designed to enable the contents on the iMac to be easily exposed as well as exfiltrated.

37. From the available forensic evidence, the unauthorized intruder maintained complete control of the system. Access to e-mails, personal files, Internet browsing, passwords, execution of programs, financial records, photographs of not just the Client but of the Client's family members was likewise achieved. With regard to attribution, information recovered directly from Plaintiff Sharyl Attkisson's computer proved that remote communication with the system was executed via at least three IP addresses owned, controlled, and operated by the United States Postal Service ("USPS"), and was not associated with any web server or website used by the USPS. Attempts to communicate with the IP addresses were rejected. These IP addresses were not randomly or accidentally logged find on Plaintiff Sharyl Attkisson's work laptop, nor were they found in the Internet browsing history because she "might have purchased stamps online." Analysis demonstrated that there was an illicit communications channel opened up between a computer on the Internet assigned with the referenced USPS IP addresses and Plaintiff Sharyl Attkisson's computer in her home, thus establishing indisputable evidence that a person using the IP address, which was under the control of the Federal government, was communicating directly with her computer on an ongoing basis during the relevant times in question.

38. In February 2012, Plaintiff Sharyl Attkisson contacted Verizon yet again to complain about continuing anomalies with her FiOS Internet, voice, and video services.

39. In March 2012, a Verizon representative visited Plaintiffs' home and replaced the router a second time. The representative also replaced the entire outside FiOS service box. Despite Verizon's efforts, however, the anomalies persisted.

40. In April and May 2012, the DOJ and FBI publicly announced a new effort to vastly expand cyber-related efforts to address alleged "national security-related cyber issues." During the same time frame, the DOJ secretly—without notice and in violation of longstanding DOJ practice—seized personal and business phone records belonging to journalists from the Associated Press news agency. The records seizure was not publicly known at the time, but was later revealed by the media.[5]

41. In July, 2012, the DOJ designated U.S. Attorneys' offices to act as "force multipliers" in its stepped-up cyber efforts in the name of national security.[6]

42. That same month, July, 2012, intruders remotely "refreshed" the ongoing surveillance of Ms. Attkisson's Toshiba computer. Again, the access was unknown to Ms. Attkisson at the time, but was revealed later through computer forensic analysis.

---

[5] See, for example, Sari Horwitz, *Under Sweeping Subpoenas, Justice Department Obtained AP Phone Records in Leak Investigation*, Washington Post, May 13, 2013, online at https://www.washingtonpost.com/world/national-security/under-sweeping-subpoenas-justice-department-obtained-ap-phone-records-in-leak-investigation/2013/05/13/11d1bb82-bc11-11e2-89c9-3be8095fe767_story.html (last accessed on Feb. 2, 2018).

[6] https://wikileaks.org/gifiles/docs/12/1210665_obama-leak-investigations-internal-use-only-pls-do-not.html (last accessed on February 2, 2018).

43. In September, 2012, Wikileaks published internal emails from a global intelligence company doing business with government agencies. The materials made reference to "Obama leak investigations" and the alleged "witch hunts of investigative journalists learning information from inside the beltway sources." The email states, "(t)here is a specific tasker from the [White House] to go after anyone printing materials negative to the Obama agenda (oh my.) Even the FBI is shocked."

44. On October 5, 2012, CBS News aired Plaintiff Sharyl Attkisson's first Benghazi story, which was critical of the Obama Administration's handling of the security requests at the U.S. compound in Benghazi, Libya, where Ambassador Christopher Stevens and three other U.S. personnel were murdered by terrorists on September 11, 2012.

45. On October 8, 2012, CBS aired another Attkisson report on Benghazi that included an interview with whistleblower Col. Andrew Wood. During the weeks following the airing of Col. Wood's interview, Plaintiff Sharyl Attkisson made personal contact with numerous confidential sources within the Federal government (or who had links to intelligence agencies within the U.S. government). The confidential government sources reported to Plaintiff Sharyl Attkisson that efforts were being made by the Obama Administration to clamp down on leaks and to track the leaking of information by Federal government employees to specific reporters regarding the Benghazi terrorist attacks.

46. During the same time period, the DOJ continued its stepped-up cyber efforts with its National Security Division, providing specialized training at DOJ headquarters for the National Security Cyber Specialists ("NSCS") network and the Criminal Division's Computer Crime and Intellectual Property Section ("CCIPS").

47. In the later part of October 2012, Plaintiffs began noticing an escalation of electronic problems at their residence in Leesburg, Virginia, including interference in home and mobile phone lines, computer interference, and digital television signal interference. However, they were still unaware of any intrusion by Defendants.

48. During the same general time frame, several sources with close ties to the US Intelligence Community privately approached Plaintiff Sharyl Attkisson and informed her that the Federal government would likely be monitoring her electronically in an effort to identify her confidential sources, and also to monitor her continued reporting on the *Fast and Furious* and *Benghazi* stories.

49. From November 7–9, 2012, Attorney General Holder hosted a national training conference at DOJ headquarters for the expanded efforts of DOJ's National Security Cyber Specialists ("NSCS").[7] On November 13, 2012, the FBI initiated several cyber

---

[7] See *New Network Takes Aim at Cyber Threat to National Security*, DOJ Blog, Nov 12, 2012, online at https://www.justice.gov/archives/opa/blog/new-network-takes-aim-cyber-threats-national-security (last accessed on Feb. 2, 2018).

> "With the network built, the [Justice] department will be able to accelerate some of the national security cyber work that has been ongoing since [National Security Division's] cyber review. To equip this large cyber cadre in how to best address these new threats, the department has developed and carried out extensive training. Last week's inaugural NSCS conference covered topics ranging from digital evidence, to the Foreign Intelligence Surveillance Act, to current threat trends, to common challenges in combating national security cyber threats specifically
>
> [T]he network will help strengthen partnerships between the department and agencies across the U.S. government, including the Department of Homeland Security, the Department of Defense, and various elements of the Intelligence Community. The network also will work particularly closely with the FBI's National Cyber Investigative Joint Task Force (NCIJTF) to help preserve all

security case investigations that would later relate to the illegal intrusions directed at Plaintiffs.

50. In November 2012, Plaintiff's phone line became nearly unusable because of anomalies and interruptions. Her mobile phones also experienced regular interruptions and interference, making telephone communications unreliable, and, at times, virtually impossible.

51. In December 2012, Plaintiff Sharyl Attkisson discussed her phone and computer issues with friends, contacts, and sources, via her home phone, mobile phones, and email. She decided to begin logging the times and dates that the computers turned on at night without her input. Soon after these phone and email discussions, the computer nighttime activity stopped.

52. Computer forensic analysis later revealed that the intruders executed remote actions in December 2012, to remove evidence of the intrusion from Plaintiffs' computers, mobile phones, and home electronic equipment.

53. In December 2012, a contact with U.S. government intelligence experience

---

> intelligence collection, prevention, disruption, and response options for cyber national security threats.
>
> Going forward, the NSCS network is focused on ensuring a whole-of-government and all-tools approach to combating cyber threats to national security. The network will be working to bring investigations and prosecutions as viable options for deterrence and disruption as part of the government-wide response to these threats. The network will also be advising and consulting other parts of the government in the use of additional tools to counter these threats."

conducted an inspection of Ms. Attkisson's exterior home. During the course of the inspection, the consultant discovered an anomaly with Plaintiffs' Verizon FiOS box: an extra fiber-optic cable was dangling from the exterior of the box.

54. Based on this odd finding, Plaintiff Sharyl Attkisson contacted Verizon on December 31, 2012. However, the Verizon customer service representative denied Verizon had installed, or had knowledge of, the extraneous fiber-optics cable affixed to the FiOS equipment at the Plaintiffs' home. Furthermore, the Verizon representative directed Plaintiffs to contact local law enforcement authorities. Shortly thereafter, a person identifying herself as a Verizon supervisor telephoned Plaintiff Sharyl Attkisson to advise her that Verizon was dispatching a service technician the next day, New Year's Day, to investigate the fiber-optic cable issue. Plaintiff Sharyl Attkisson informed the purported Verizon supervisor that it was unnecessary to dispatch a technician just on a holiday, and she offered to send Verizon a photograph of the fiber-optic cable to save Verizon the trip. However, the supervisor declined the photograph and insisted that a technician would be present on New Year's Day.

55. On January 1, 2013, a person representing himself to be a Verizon technician visited Plaintiffs' home and removed the additional fiber-optic cable dangling from the outdoor FiOS box. Plaintiff Sharyl Attkisson asked the technician to leave the cable. The technician placed it next to the equipment and left the home. When Plaintiff Jim Attkisson arrived home and went to retrieve the extraneous cable, the cable had already been removed and was no longer on the premises.

56. Throughout the month of January 2012, Plaintiff Sharyl Attkisson repeatedly

contacted the purported Verizon service technician to seek the location of the missing cable. The person representing himself as a technician never returned any of the calls at the number he had provided.

57. In January and February of 2013, Plaintiffs continued to experience phone and Internet usage issues, including drop-offs, noises, and other interference. Verizon was notified by Plaintiffs of these service issues, and technicians and supervisors made additional contacts and visits.

58. On January 8, 2013, Plaintiff Sharyl Attkisson made arrangements to deliver her Toshiba work laptop to an individual with special expertise in computer forensics. On January 9, 2013, the forensics expert reported to Plaintiff Sharyl Attkisson that her work laptop showed clear evidence of outside and unauthorized "intrusion," and that the source of the intrusion and electronic surveillance was likely the US government due to the sophisticated nature of the technology used.

59. On January 10, 2013, the work laptop was returned to Plaintiff Sharyl Attkisson, along with a report. According to the report, the forensics computer expert found that sophisticated malicious software ("malware") had been used to accomplish the intrusion, and the software fingerprint indicated the malware was proprietary to the Federal government. The intrusion included, among other types of electronic surveillance, keystroke monitoring, exfiltration of data, audio surveillance of Plaintiff's conversations and activities at home by activating Skype, mining personal passwords, monitoring work and personal email, and likely compromise of Plaintiffs' work and personal smartphones.

60. According to the report, the electronic surveillance by the identified malware

spanned most of 2012, at least. The report also stated the intruders had accessed CBS's internal networks, computer systems, and enterprise software applications, such as the ENPS program, and that the perpetrator had also placed three (3) classified documents deep in the computer's operating system. Plaintiff Sharyl Attkisson thereafter notified her direct supervisor at CBS News of the laptop intrusion and findings.

61. On February 2, 2013, an independent forensic computer analyst retained by CBS News spent approximately six (6) hours at Plaintiffs' home, during which time he reported finding evidence on both Plaintiff Sharyl Attkisson's work laptop and personal Apple iMac desktop computers of a coordinated, highly-skilled series of actions and cyber-attacks directed at the operation of the computers and the storage and access of data thereon. CBS engaged the company to do further analysis of the work laptop in an attempt to recover wiped data and determine the methods used compromise the system.

62. In March 2013, Plaintiff Sharyl Attkisson's Apple iMac desktop computer began malfunctioning and, after several days of it freezing and emitting a burning odor, it shut down. She was unable to turn the Apple computer back on after this event.

63. On April 3, 2013, Plaintiff Sharyl Attkisson filed a complaint with the DOJ Inspector General regarding the incidents of electronic surveillance and cyber-stalking described above.

64. On May 6, 2013, an official with the DOJ's Inspector General ("IG") office called Plaintiff Sharyl Attkisson and stated that he had checked with the FBI, and the FBI denied any knowledge of any operations concerning her computers or phone lines. The DOJ

IG official also stated that there was no Foreign Intelligence Surveillance Act ("FISA") or PATRIOT Act related order authorizing electronic surveillance against her.

65. On May 21, 2013, Plaintiff Sharyl Attkisson publicly stated in a radio interview her belief that her computers had been compromised, but did she not assign or allege responsibility. Subsequently, a news outlet sought a statement from the DOJ regarding Plaintiff Sharyl Attkisson's assertions. The DOJ issued a written response stating, "To our knowledge, the Justice Department has never compromised Ms. Attkisson's computers, or otherwise sought any information from or concerning any telephone, computer or other media device she may own or use."

66. On June 10, 2013, the independent cyber-security firm hired by CBS confirmed that there was a highly sophisticated intrusion into Plaintiff Sharyl Attkisson's work laptop. Moreover, the firm discovered that in December 2012, the perpetrators of the cyber-attacks initiated "clean-up" actions from a computer at a remote location on the Internet in an attempt to delete all evidence from the work laptop of the intrusion and electronic surveillance.

67. On June 11, 2013, CBS News issued a public statement, based on the forensics report from the independent cyber-security firm, confirming that Plaintiff Sharyl Attkisson's work laptop was accessed by an unauthorized, external, unknown party on multiple occasions in late 2012, and that the party used sophisticated methods to attempt to remove all possible indications of unauthorized activity.

68. The DOJ Inspector General requested a copy of the CBS forensic expert's report and requested the opportunity to examine the work laptop. However, CBS denied the

DOJ IG's requests. Plaintiff Sharyl Attkisson then retained a separate independent computer forensics expert to conduct further analysis of her work laptop.

69. In September 2013, while Ms. Attkisson continued working on the *Benghazi* story at her home in the evening, she observed for the first time that a third computer, her personal Apple MacBook Air, was accessed remotely, controlled by unknown attackers, and had data accessed and deleted.

70. In June 2013, though Plaintiffs were unaware at the time, the Defendants had begun conducting inquiries Plaintiff Sharyl Attkisson's computer intrusions under the auspices of a national security issue, but both DOJ and the FBI failed to contact or interview Plaintiffs. Plaintiff Sharyl Attkisson only discovered the FBI inquiry in December 2013, when she appealed the denial of her Freedom of Information Act ("FOIA") request to the FBI and received some responsive documents.[8]

71. The FBI investigation involving Plaintiff Sharyl Attkisson's computer intrusions was circulated to the DOJ's national cyber-security group and included with a set of cases opened in November 2012, during the DOJ's expansion of its cyber team and the announcement of its intention to use "new tools" in its arsenal.

72. Although CBS did not release the compromised work laptop to the DOJ IG, in January 2014, Plaintiff Sharyl Attkisson agreed to release her personal Apple iMac desktop computer to the DOJ IG for analysis. During the investigation, the investigators

[8] Plaintiffs were unaware of the FBI case at the time it was opened and for months thereafter.

remarked to the Plaintiff that they saw a great deal of suspicious activity on the computer.

73. However, as months went by, the DOJ IG refused to release a written report to Plaintiffs. The DOJ IG also failed to properly respond to Plaintiff Sharyl Attkisson's subsequent FOIA requests on the topic. The DOJ IG finally released a partial report upon Congressional request on the eve of Plaintiff Sharyl Attkisson's testimony to a Senate panel in early 2015. Although the report summary noted a great deal of advanced-mode computer activity not attributable to Plaintiffs, the report nonetheless concluded, paradoxically, that DOJ IG found no evidence of intrusion into her personal Apple iMac computer. The DOJ IG report was provided by government officials to the press. However, the report did not examine the compromised CBS laptop computer.

74. On January 16, 2014, and January 27, 2014, the head of the DOJ IG Computer Forensics unit and a colleague visited Plaintiffs' home as part of the investigation, which included analysis of the Apple iMac desktop.

75. Between 2015 and 2017, additional forensic analysis of Plaintiff Attkisson's CBS work laptop identified three (3) US Postal Service ("USPS") Internet Protocol ("IP") addresses used in the Advanced Persistent Threat ("APT")[9] cyber-attacks, electronic

---

[9] See National Institute of Standards and Technology ("NIST"), *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 *B–1 (Mar 2011).

> An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission,

surveillance, data exfiltration, and cyber-stalking against Plaintiff by the US government between 2010 and 2014.

76. Specifically, USPS-owned IP version 4 ("IPv4") addresses 56.91.143.9 and 56.189.149.2, and IP version 6 ("IPv6") address 385b:8f09:80fa:ffff:385b:8f09:80fa:ffff, were used as part of a "zero-day" attack against Plaintiff's work laptop (running Microsoft's Windows 7 Professional).[11] The attackers leveraged a previously unknown software vulnerability in Intel Corporation's Active Management Technology ("AMT") software[12] to exploit Plaintiff's laptop remotely using at least three USPS IP addresses. Forensic evidence also shows that Defendants Verizon Business Services, Verizon Wireless, and Verizon–VA ("Verizon Defendants") supported the use of these same USPS-owned IP addresses on their respective wireline and wireless networks to enable the US government's electronic surveillance and data exfiltration against Plaintiff Attkisson.

77. Only the FBI has both the necessary legal authorities and the resources to conduct an APT-style cyber-attack such as this in the United States against Plaintiffs—focusing on Plaintiff Sharyl Attkisson, a US person ("USP") and member of the

---

program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

[11] According to the US Government's Committee on National Security Systems ("CNSS"), a zero-day attack "exploits a previously unknown hardware, firmware, or software vulnerability". See *Committee on National Security Systems (CNSS) Glossary*, Apr 5, 2015, online at https://csrc.nist.gov/Glossary/?term=2541.

[12] See *About the Intel Manageability Firmware Critical Vulnerability*, May 26, 2017, online at https://www.intel.com/content/www/us/en/architecture-and-technology/intel-amt-vulnerability-announcement.html

news media—using a zero-day vulnerability in combination with multiple IP addresses owned by the USPS. Moreover, during the entire period of the APT cyber-attack, Defendant Verizon Business Services and Defendant Verizon Wireless were also providing bulk metadata to the FBI, including metadata from Plaintiff Sharyl Attkisson's CBS mobile phone, personal home phone, and personal home Internet connection.

78. Analysis conducted by Plaintiffs' forensic experts also indicates that the FBI's Digital Collection System ("DCS") electronic surveillance capabilities deployed on Defendant Verizon Business Services' landline networks and Defendant Verizon Wireless' wireless networks by the FBI's Telephone Telecommunications Intercept and Collection Technology Unit ("TICTU") of the Operational Technology Division ("OTD") based at—including TICTU's DCS-3000, NG–DCS–5000, and DCS–6000 platforms—were subverted and compromised by the Defendants as part of the overall APT cyber-attacks, electronic surveillance and cyber-stalking against Plaintiffs.

79. According to the Obama Administration's 2014 budget submission to Congress, the TICTU's DCS platforms "will continue to collect 100% of Title 50 and Title III collection data, as well as support all new and existing Title 50 and Title III collection system users."

80. From an operational perspective, TICTU's DCS platforms support, among other things, the "incidental" collection of metadata and content related to US persons.

81. Here, TICTU's DCS platforms including service-oriented architecture ("SOA") middleware interfacing, respectively, with Defendant Verizon Business Services' and Defendant Verizon Wireless' switches, routers, and network elements—were subverted

and compromised by DOJ and the FBI as part of the overall APT cyber-attacks and cyber-stalking against Plaintiffs.

82. The forensic analysis likewise confirms that agents or employees of Defendants were likewise involved in the tapping of Plaintiffs' FiOS fiber-optic telecommunication line, and a mobile WiFi hot-spot (Verizon MiFi 4510L) provisioned on Defendant Verizon Wireless' network was used to connect to Plaintiff Sharyl Attkisson's work laptop for surveillance and data exfiltration by the U.S. government using Defendant Verizon Wireless' resources; and Defendants used an Inmarsat BGAN mobile satellite terminal to connect to Plaintiff Sharyl Attkisson's work laptop for surveillance and data exfiltration.

83. Finally, forensic evidence points directly at the Verizon Defendants—through a combination of their respective employees and resources—as having knowingly and willingly assisted in the U.S. government's subversion of Title III, Title 50, and Executive Order 12333 legal authorities, and the technical collection capabilities associated with them—for political purposes, including, but not limited to, the unmasking of Plaintiff Sharyl Attkisson's identity in intelligence reports in violation of her Fourth Amendment rights.

84. In carrying out the APT cyber-attacks against Plaintiffs, including electronic surveillance and cyber-stalking, the Defendants' conduct including the following items:

A. The Internet is a network of interconnected networks. Information is shared between these networks, in the form of Internet Protocol ("IP") packets, using routers. IP packets follow a path of routers from their source to their destination.

B. Here, between January 4, 2013, and January 8, 2013, among other relevant time periods, Defendants used a remote system, assigned with US Postal Service ("USPS") IPv4 address 56.91.143.9 and USPS IPv6 address 385b:8f09:80fa:ffff:385b:8f09:80fa:ffff, to communicate using transmission control protocol ("TCP") with Plaintiff Sharyl Attkisson's work laptop.

C. Defendants' remote system was used for both command and control and data exfiltration in the electronic surveillance and cyber-stalking against Plaintiffs.

D. During the referenced five days, among other relevant time periods, Plaintiff Sharyl Attkisson's work laptop was in her Leesburg, Virginia, home and connected to the Internet through Defendant Verizon–VA's FiOS Internet service.

E. The USPS IP addresses were logged automatically on Plaintiff Sharyl Attkisson's work laptop by a software application called evteng.exe, a component of Intel's wireless networking management software, and a resource owned, operated and controlled by Defendants.

F. Routers are collectively responsible for maintaining paths, or routes, to all reachable destinations on the Internet. Reachability information is shared between routers by routing protocols. As traffic is received at a router, it is forwarded based on the reachability information stored in the router's forwarding table, and other information stored in the IP packet's header. A group of routers under the same administrative control is considered an Autonomous System ("AS") and is designated by an Autonomous System Number ("ASN"). For example, in October 1995, according to the American Registry for Internet Numbers ("ARIN"), USPS's group of Internet-connected routers was designated

with ASN AS5774. To communicate between ASNs, routers perform inter-domain routing using an external gateway protocol ("EGP"). The primary EGP in use on the Internet during the relevant time period was Border Gateway Protocol version 4 ("BGPv4").

G. In October 2017, during deposition testimony by USPS technical representative Cliff Biram, USPS testified that IP address 56.91.143.9, among others, was never advertised by USPS—using BGPv4 or any other EGP method—on the Internet.

H. Analysis by Plaintiffs' Forensic Team indicates that, between 2007 and 2014, BGP hijacking incidents occurred at U.S. and European Internet service providers ("ISPs") involving the unauthorized advertising on the Internet of USPS's entire Class A block of 16,777,216 IPv4 addresses, or USPS's entire 56.0.0.0/8 IPv4 prefix. Specifically, the following ASNs in the U.S. and Europe were involved in BGP hijacking incidents that included, among others, USPS IPv4 prefix 56.91.143.0/24 (including IPv4 address 56.91.143.9) and USPS IPv4 prefix 56.189.149.0/24 (including IPv4 address 56.189.149.2):

a. AS701 (Verizon Business);
b. AS702 (Verizon Business);
c. AS703 (Verizon Business);
d. AS3303 (Swisscom Ltd, Switzerland);
e. AS3352 (Telefonica de Espana, Spain)
f. AS7046 (Verizon Business);
g. AS2634 (Verizon Wireless);
h. AS6167 (Verizon Wireless);
i. AS6265 (Verizon Wireless);
j. AS12079 (Verizon Wireless);
k. AS12956 (Telefonica International Wholesale Services, Spain);
l. AS15469 (Warinet Global Services SA, Switzerland);
m. AS17106 (Verizon Wireless); and,
n. AS22394 (Verizon Wireless);
o. AS29222 (Infomaniak Network SA, Switzerland);
p. AS35054 (Equinix Enterprises GMBH, Switzerland); and,
q. AS39202 (GCap Media PLC, United Kingdom).

I. Thus, although in January 2013 USPS was not advertising the IP addresses that were logged on Plaintiff Sharyl Attkisson's work laptop, these IP addresses were in fact being used by government resources, including Defendants.

J. As mentioned above, Plaintiff's Forensic Team discovered that *malware* files running on Plaintiff Sharyl Attkisson's work laptop, including while it was connected via a Juniper VPN link to CBS's internal corporate network at her home in Leesburg, Virginia, were using the USPS IPv4 and IPv6 addresses to communicate across Verizon's FiOS network with one or more remote systems controlled by the Defendants.

K. The malware files were recovered from a forensic image of the laptop's internal hard drive by using Arsenal Recon software to carve the hiberfil.sys file, and, subsequently, by using Volatility 2.6 software to carve the ActiveMemory.bin file that was extracted from the hiberfil.sys file. These operating system files were created by Microsoft's Windows 7 Professional operating system on January 8, 2013, when the laptop went into hibernation mode. On January 8, 2013, there were 1,652 dynamic-link library ("DLL") files running in memory on Plaintiff Sharyl Attkisson's work laptop.

L. In addition, Plaintiff's Forensic Team discovered that another 525 of the 1,652 DLL files running on the work laptop have a malicious confidence score between 60% and 90% on VirusTotal.

M. The following security events were logged by Facebook and Wikipedia between January 2013 and March 2014. These events indicate electronic surveillance and cyber-stalking against Plaintiff Sharyl Attkisson's Facebook social media accounts,

@sharyl.attkisson and @sharylattkissonpublic, and her Wikipedia page, https://en.wikipedia.org/wiki/Sharyl_Attkisson, originating from her Verizon FiOS residential Internet connection or her Verizon Wireless work mobile phone, Mobile Station International Subscriber Directory Number ("MSISDN") +1-202-365-8509, respectively, each attributable to the same US government activities and resources set forth above.

a. At 2142 EST on February 27, 2013; 1509 EST on March 2, 2013; 2351 EST on April 16, 2013; 2239 EST on June 7, 2013; 1652 EST on June 10, 2013; 2159 EST and 2200 EST on July 27, 2013; 2307 EST on August 30, 2013; 1612 EST on September 20, 2013; and 1852 EST on October 12, 2013, Facebook logged security-related events, respectively, against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 96.241.87.96;
b. According to the ARIN, on December 29, 2006, IP address 96.241.87.96 was assigned to MCI Communications Services, Inc. d/b/a Verizon Business; the DNS entry for this IP address is pool-96-241-87-96.washdc.fios.verizon.net; and the ASN associated with this IP address is: AS701;
c. At 1445 EST on October 14, 2014, Facebook logged a security-related event against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 96.255.234.210;
d. According to the ARIN, on December 29, 2006, IP address 96.255.234.210 was assigned to MCI Communications Services, Inc. d/b/a Verizon Business; the DNS entry for this IP address is pool-96-255-234-210.washdc.fios.verizon.net; and the ASN associated with this IP address is: AS701.
e. At 0014 EST on May 9, 2014, Facebook logged a security-related event against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 108.18.98.113;
f. According to ARIN, on June 5, 2009, IP address 108.18.98.113 was assigned to MCI Communications Services, Inc. d/b/a Verizon Business; the DNS entry for this IP address is pool-108-18-98-113.washdc.fios.verizon.net; and the ASN associated with this IP address is: AS701.
g. At 2215 EST on January 23, 2013, Facebook logged a security-related event against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 108.45.139.237;

h. Between August 12, 2012, and September 27, 2012, Wikipedia logged edits made to Plaintiff Sharyl Attkisson's Wikipedia page that were originating from IP address 108.45.139.237;
i. According to the ARIN, on June 5, 2009, IP address 108.45.139.237 was assigned to MCI Communications Services, Inc., d/b/a Verizon Business; the DNS entry for this IP address is pool-108-45-139-237.washdc.fios.verizon.net; and the ASN associated with this IP address is: AS701.
j. At 2318 EST on December 10, 2013, and 2002 EST on January 24, 2014, Facebook logged, respectively a security-related event against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 173.73.91.181;
k. According to ARIN, on August 11, 2008, IP address 173.73.91.181 was assigned to MCI Communications Services, Inc. d/b/a Verizon Business; the DNS entry for this IP address is pool-173-73-91-181.washdc.fios.verizon.net; and the ASN associated with this IP address is: AS701;
l. At 2222 EST on October 1, 2013, Facebook logged a security-related event against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 174.236.97.12;
m. According to ARIN, on December 16, 2008, IP address 174.236.97.12 was assigned to Cellco Partnership, d/b/a Verizon Wireless; the DNS entry for this IP address is 12.sub-174-236-97.myvzw.com; and the ASN associated with this IP address is: AS22394;
n. At 2156 EST on June 10, 2013, Facebook logged a security-related event against Plaintiff Sharyl Attkisson's Facebook account that was originating from IP address 174.252.112.169; and,
o. According to ARIN, on December 16, 2008, IP address 174.252.112.169 was assigned to Cellco Partnership, d/b/a Verizon Wireless; the DNS entry for this IP address is 169.sub-174-252-112.myvzw.com; the ASN associated with this IP address is: AS6167.
p. Between 2011 and 2014, Plaintiff Sharyl Attkisson logged numerous events during which her work mobile phone (an Apple iPhone, phone number 202-365-8509, that was provisioned on Verizon Wireless's network) or her personal mobile phone (a BlackBerry Curve, phone number 202-684-0038, that was provisioned on T-Mobile's network) were subjected to severe radio-frequency ("RF") interference. These events were likewise attributable to Defendants by virtue of the same modes and methods described above.
q. Verizon provided the government defendants with an end-to-end path between the Plaintiff's home in Leesburg, Virginia, and the FBI's cyber processing facility in Quantico, Virginia.

85. The above-cited events, which offer only brief highlights of the cyber-attacks suffered in Plaintiffs' home or at Plaintiff Sharyl Attkisson's office at CBS News, caused Plaintiffs to incur unreasonable and unnecessary expenses in an effort to diagnose and correct the problems resulting from the attacks and intrusions; resulted in an invasion of their personal and family privacy; caused them to fear for their individual and family's well-being and safety; interfered with their ability to use their telephones, computer, and television; caused them fear for her sources' well-being and safety; interfered with Plaintiffs' ability to maintain necessary contacts with sources to perform her professional investigative reporting duties as a member of the press; affected Plaintiffs' sources' willingness to communicate with her; distracted from her duties as an investigative reporter; and resulted in irreparable tension in her relationship with her employer.

86. The actions of personnel working on behalf of the Defendant United States as described above, including the government intrusions, negligently, recklessly, and intentionally caused Plaintiffs' rights to privacy to be violated, and trespassed upon Plaintiffs' real and personal property as alleged herein, without probable cause or any other legal justification, and as a result, Plaintiffs suffered damages.

87. The actions of the government employees and/or agents constitute violations of applicable law. Under the FTCA, the United States of America is liable for misconduct and actions of its agents and employees.

88. Defendants acted under color of law when conducting surveillance on the Plaintiffs and inhibiting the exercise of their First Amendment rights.

89. The surveillance of Plaintiffs' computers and telephones violated the

Plaintiffs' right to privacy and trespassed upon their real and personal property. By subjecting Plaintiffs to surveillance of Ms. Attkisson's investigative efforts, Defendants sought to abridge the freedom of the press and chill the exercise of the Plaintiffs' free speech in a reckless manner with objective unreasonableness, and with the intent to violate their rights.

90. The violation of Plaintiffs' right to privacy, and Constitutional rights, and the trespass upon Plaintiffs' real and person property proximately caused injuries, as set forth herein.

91. At all times relevant to the subject Complaint, the Defendants acted with reckless and callous indifference to the rights of Plaintiffs with the intent to subject them to, or cause them to be subjected to, constitutional violations.

COUNT 1
VIOLATION OF THE FIRST
AMENDMENT TO THE CONSTITUTION

92. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein, including the allegation of the original complaint.

93. This action arises under *Bivens.*[13]

94. Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America acted under color of law when conducting surveillance on the Plaintiffs and inhibiting the exercise of her First Amendment rights.

---

[13] See footnote 1.

95. The surveillance of Plaintiffs' computers and telephones violated the First Amendment to the United States Constitution. By subjecting Plaintiffs to surveillance of her investigative efforts, Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America sought to abridge the freedom of the pressand chill the exercise of her free speech in a reckless manner with objective unreasonableness, and with the intent to violate their rights.

96. The violation of Plaintiffs' First Amendment rights proximately caused injuries, as set forth herein.

97. By virtue of the foregoing, the Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America are liable to Plaintiffs for the violation of rights under the First Amendment.

COUNT 2
VIOLATION OF THE FOURTH AMENDMENT TO THE CONSTITUTION

98. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein, including all allegations in the original complaint.

99. As before, this action arises under *Bivens.*[14]

100. At all times relevant to the subject Complaint, Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America acted under color of law when conducting surveillance on the Plaintiffs.

101. The surveillance of Plaintiffs' computers and telephone violated the Fourth

[14] See footnote 1.

Amendment to the United States Constitution. The Plaintiffs' right to be secure in their person, residence, papers, and effects against unreasonable searches and seizures was violated. The Plaintiffs had a reasonable expectation of privacy with respect to their computers and telephones, and the Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America had no warrant authorizing the surveillance, nor did any exigent circumstances exist at the time of such surveillance.

102. The violation of the Plaintiffs' Fourth Amendment rights proximately caused their injuries, as set forth herein.

103. The Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America acted with reckless and callous indifference to the federally protected rights of the Plaintiffs. Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America's conduct, among other things, included all actions set forth in paragraph 71 above. That paragraph, including all sub-paragraphs, are hereby incorporated by reference as if repeated in this Count.

104. By virtue of the foregoing, the Defendants Unknown Named Agents of the Department of Justice, United States Postal Service, and United States of America are liable to Plaintiffs for their violation of the Plaintiffs' rights under the Fourth Amendment.

COUNT 3
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVCAY ACT
18 U.S.C. §§ 2511 & 2520

105. All prior allegations are restated herein by reference.

106. The Defendants, individually and in concert, intercepted, endeavored to intercept, and/or procured another person to intercept or endeavor to intercept the Plaintiffs' wire, oral, or electronic communications.

107. The Defendants, individually and in concert, used, endeavored to use, and/or procured another person to use or endeavor to use an electronic, mechanical, or other device to intercept Plaintiffs' oral communications. Such device or devices were affixed to or transmitted a signal through a wire used in wire communications, and was for the purpose of obtaining information relating to business which affects interstate commerce. A substantial part of such conduct occurred in the District of Columbia.

108. The Defendants, individually and in concert, disclosed or endeavored to disclose the contents of Plaintiffs' wire, oral or electronic communications, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communications.

109. Upon information and belief, the above alleged conduct occurred without authorization from a court of competent jurisdiction.

110. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

COUNT 4
VIOLATION OF THE STORED COMMUNICATIONS ACT
18 U.S.C. §§ 2701 & 2707

111. All prior allegations are restated herein by reference.

112. The Defendants, individually and in concert, intentionally accessed and/or caused to be accessed without authorization a facility through which an electronic

communication service is provided, and thereby obtained Plaintiffs' wire or electronic communications while they were in electronic storage.

113. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

COUNT 5
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
18 U.S.C. § 1030

114. All prior allegations are restated herein by reference.

115. The Defendants, individually and in concert, intentionally accessed the Plaintiffs' computers and thereby obtained information from a protected computer, to wit Ms. Attkisson's computers used for her work as an investigative journalist for a national news agency.

116. The Defendants, individually and in concert, knowingly and intentionally accessed and/or caused to be accessed Plaintiffs' protected computers, causing interruption and interference with the ability to use such computers.

117. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

COUNT 6
VIOLATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT
50 U.S.C. § 1810

118. All prior allegations are restated herein by reference.

119. The Plaintiffs were the target of electronic surveillance and/or their communications were subject to electronic surveillance at the hands or direction of the

Defendants, and therefore qualify as "aggrieved persons" per 50 U.S.C. § 1801.

120. The Plaintiffs were not provided with notice of such surveillance, and upon information and belief such surveillance was not conducted pursuant to authorization from a court of competent jurisdiction.

121. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

COUNT 7
VIOLATION OF THE VIRGINIA COMPUTER CRIMES ACT
VA. CODE § 18.2-152.12

122. All prior allegations are restated herein by reference.

123. The Defendants, individually and in concert, caused the Plaintiffs' computers to malfunction, and used or caused to be used a computer or computer network to make or cause to be made an unauthorized copy of data and communications stored in the Plaintiffs' computers.

124. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

COUNT 8
COMMON LAW TRESPASS TO LAND AND CHATTEL

125. All prior allegations are restated herein by reference.

126. The Defendants, individually and in concert, entered upon or caused others to enter upon the Plaintiffs' property for purposes of installing unauthorized wire surveillance devices to conduct unlawful surveillance upon the Plaintiffs' electronic communications.

127. The Defendants, individually and in concert, intruded upon or caused others to intrude upon the Plaintiffs' personal property, namely computers and other electronic devices, for purposes of conducting unlawful surveillance upon the Plaintiffs' electronic communications.

128. These trespasses to land and chattel were conducted without the Plaintiffs' consent and without lawful authority.

129. As a result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

DAMAGES

130. The Defendants' conduct directly and proximately caused injury to the Plaintiffs in the form of trespass upon and damage to personal property, both real and tangible, workplace harassment and intimidation, fear, stress, embarrassment, expense, inconvenience, and anxiety.

131. In an effort to discover what was happening with Plaintiff Sharyl Attkisson's work laptop and phone lines, the Plaintiffs were forced to spend a substantial amount of time and expense in investigating the maladies and hiring others to perform forensic investigations.

132. As a journalist, the ability to protect sources is crucial, and Plaintiff Sharyl Attkisson's ability to offer such protection was compromised as a result of the surveillance giving rise to this claim.

133. This created a substantial amount of anxiety, jeopardized Plaintiff Sharyl Attkisson's success as a journalist, and made her job more difficult than it would otherwise

have been.

134. Plaintiffs have incurred and will continue to incur attorneys' fees for the prosecution of this action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request judgment in their favor against Defendants United States of America, Federal Bureau of Investigation, MCI Communications Services, Inc. d/b/a Verizon Business Services, Cellco Partnership d/b/a Verizon Wireless, Unknown Named Agents of the Department of Justice, Unknown Named Agents of the United States Postal Service, and Unknown Named Agents of the United States, jointly and severally, for compensatory damages in an amount to be proven at trial; for punitive damages in an amount to be proven at trial; for statutory damages pursuant to 18 U.S.C. §§ 1030, 1810, 2520 & 2707, and Virginia Code § 18.2-152.12; for an injunction prohibiting the Defendants, and all other agents of the U.S., DOJ and USPS, from conducting surveillance of any sort against Plaintiff Sharyl Attkisson without first obtaining a warrant in compliance with the law; for a Declaration that Defendants' actions, practices, customs, and policies regarding the unauthorized surveillance of the Plaintiffs were unjustified, illegal, and violated the constitutional and legal rights; for attorney's fees and costs; and for such other and further relief as the Court may deem just and appropriate.

TRIAL BY JURY IS DEMANDED.

Respectfully Submitted,
SHARYL THOMPSON ATTKISSON
JAMES HOWARD ATTKISSON
SARAH JUDITH STARR ATTKISSON
By counsel

/s/ J. Gregory Webb
J. Gregory Webb, Esq. (VA Bar No. 38157)
David W. Thomas, Esq. (VA Bar No. 73700)
E. Kyle McNew, Esq. (VA Bar No. 73210)
MichieHamlett PLLC
500 Court Square, Suite 300
Post Office Box 298
Charlottesville, VA 22902-0298
Phone: (434) 951-7200
Fax: (434) 951-7218
dthomas@michiehamlett.com
gwebb@michiehamlett.com
kmcnew@michiehamlett.com

C. Tab Turner, Esq. (Admitted *Pro Hac Vice*)
TURNER & ASSOCIATES, P.A.
4705 Somers Avenue, Suite 100
North Little Rock, Arkansas 72116
501-791-2277 – Office
501-791-1251 – Facsimile
Tab@TTurner.com

CERTIFICATE OF SERVICE

I hereby certify that on February 5, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing (NEF) to the following counsel of record:

Andrew Han, Esq.
Dennis Carl Barghaan, Jr., Esq.
Office of the United States Attorney
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314
Tel: 703-299-3970
Fax: 703-299-3983
Andrew.han@usdoj.gov
Dennis.barghaan@usdoj.gov

/s/ J. Gregory Webb

J. Gregory Webb, Esq. (VA Bar No. 38157)
David W. Thomas, Esq. (VA Bar No. 73700)
E. Kyle McNew, Esq. (VA Bar No. 73210)
MichieHamlett PLLC
500 Court Square, Suite 300
Post Office Box 298
Charlottesville, VA 22902-0298
(434) 951-7200; (434) 951-7218 (Facsimile)
dthomas@michiehamlett.com
gwebb@michiehamlett.com
kmcnew@michiehamlett.com